REMARKS

Applicants have studied the Final Office Action dated October 1, 2007 and have made amendments to claims 1, 7, 10, 15, and 20. No new matter was added. Reconsideration and allowance of the pending claims in view the following remarks are respectfully requested. Applicants submit that the application is in condition for allowance. In the Office Action, the Examiner:

- Rejected claims 1-22 under 35 U.S.C. § 103(a) as being unpatentable over Circenis (U.S. Patent Publication 2004/0054908 in view of the OpenPGP Standard (RFC 2440) further in view of The IBM Certification Study Guide AIX V4.5 System Administration (1999).

Rejections under 35 U.S.C. § 103(a)

As noted above, the Examiner rejected claims 1-22 under 35 U.S.C. § 103(a) as being unpatentable over Circenis (U.S. Patent Publication 2004/0054908 in view of the OpenPGP Standard (RFC 2440) further in view of The IBM Certification Study Guide AIX V4.5 System Administration (1999).

In particular, independent amended independent claim 1 now more clearly recites:

> A system that allows analysis of software running in a tamper- resistant environment, the system comprising:
>
> a processor which monitors at least one instance of software execution, wherein the one instance is identified and selected by an end-user to be monitored by the processor, wherein the end-user is a user that initiates execution of the software at a system associated with the user, and wherein the processor creates a log entry with at least one set of data derived from the one instance of software execution in response to the one instance being identified and selected to be monitored, whereby the set of data is used to diagnose the software execution;
>
> an encryption system which generates at least one symmetric key and encrypts the log entry for the at least one set of data using the symmetric key,

wherein the encryption system encrypts the symmetric key using a public key associated with the encryption system;

a log file of a relatively-fixed size which stores the log entry for the at least one set of data which has been encrypted, and wherein the log file includes the symmetric key which has been encrypted with the public key;

random data in the log file when it is originally created and which is replaced by log entries so that a size of the log file including log entries appears to be a substantially constant size; and

a pointer which identifies a next storage location for a next log entry so that a last log entry can be determined and the next log entry can be positioned in a location in the log file after a previous log entry.

The Examiner states the "Response To Arguments" section on page 2 of the present office action:

> The Applicant argues that "a 'user' in the presently claimed invention is completely different from a "sender" as taught by Circenis. As expressly taught by Circenis, the sender is the data owner... whereas a user in the presently claimed invention is an end user or an IT professional (pg. 14-15 of Remarks)." The Examiner notes that although the Applicant has clarified the definition of "user" in the Remarks, the claim language has not been amended. As such, "a user" may broadly be interpreted as a "data owner" as well as a customer.

The Applicants have amended claim 1 (and claims 10, 15, and 20) to more clearly recite:

> [...]
> a processor which monitors at least one instance of software execution, wherein the one instance is identified and selected by an end-user to be monitored by the processor, wherein the end-user is a user that initiates execution of the software at a system associated with the user
> [...]

As can be seen, claim 1 now clearly distinguishes between a data owner as taught by Circenis and an end-user such as a customer as recited for claim 1. Nowhere does Circenis teach or suggest that the end-user selects a particular instance of software execution for monitoring. In fact, the entire focus of Circenis is to detect end-user tampering of usage data. The data owner of Circenis configures an application to monitor every instance of an application use, CPU operation, or whatever data is being collected. The presently claimed invention, on the other, hand, is only monitoring a specific instance of a software execution that has been selected by the

end-user.

The Examiner goes on to state on pages 4-5 of the present Office Action that Circenis teaches "a processor which monitors at least one instance of software execution identified and selected by a user to be monitored and creates a log entry with at least one of a set of data is used to diagnose the software execution". The Examiner supports this assertion by stating Circenis teaches "[u]sing the tamper-evident system 200 of FIG. 3, a sender is able to monitor and control application utilization by collecting data associated with the application, creating tamper-evident data records, and providing the tamper-evident data records" (Circenis at paragraph [0037]).

The Applicants believe that the arguments made in the previous Response With Amendment are applicable here in view of the above amendments and respectfully request that the Examiner reconsider these arguments. As expressly taught by Circenis, the sender is the data owner (See Circenis, for example, at paragraph [0018]), whereas a user in the presently claimed invention is an end user or an IT professional. In other words, Circenis is directed at monitoring content usage and tampering of content control policies (See Circenis generally), while the present invention is directed at debugging an application running within a protected environment (See the Specification as originally filed at, for example, pages 3, 7, and 14).

The customer of Circenis is more comparable to the user of the presently claimed invention, where the customer of Circenis is actually using the application, music file, etc. Nowhere does Circenis teach or suggest "a processor which monitors at least one instance of software execution identified and selected by a user to be monitored" (emphasis added). In fact, Circenis teaches away from this claim element. The entire purpose of Circenis is to detect any tampering of a file by a user. Therefore, if a user was given the ability to turn on/off logging as recited for the presently claimed invention, the tamper-evident management system in Circenis would be defeated.

The monitoring of the presently claimed invention is only performed on the instances selected by

the end-user. Circenis is completely silent on this claim element. For example, Circenis teaches a metering application that collects "metrics data associated with operation of the computer system" whenever a user uses an application. See Circenis at paragraph [0019]. If a user uses an application 5 times, Circenis teaches that usage information for each of the 5 times is recorded. Assuming arguendo that Circenis and the presently claimed invention teaches logging and monitoring the same type of data (which they do not), Circenis would have to teach that of the 5 times an application is used a user can select which of the 5 times data should be logged. Circenis clearly does not teach this. In fact, this is completely against what Circenis is trying to accomplish as stated above. Accordingly, the presently claimed invention distinguishes over Circenis for at least this reason.

Additionally, claim 1 also recites "...whereby the set of data is used to diagnose the software execution..." The Applicants are unsure of how the Examiner concluded that Circenis teaches this element. Circenis records metrics for pay-per-use data and/or DRM usage data. Nowhere does Circenis teach that this data is used to diagnose the software execution. Accordingly, the presently claimed invention distinguishes over Circenis for at least this reason as well.

Furthermore, dependent claim 7 (and similarly claims 11, and 16) now more clearly recites "wherein the system further includes a mechanism for receiving an input from an end-user that initiates logging of log entries into the log file each time logging is desired by the user". The Examiner in the "Response To Arguments" section on page 3 of the present Office Action states that:

> "The Examiner is simply suggesting that the vendor initiates the logging of data. ("The vendor would likely want a method for accounting and auditing usage to ensure that the customers were not tampering'with the CPU usage data" Paragraph [0023]). The Examiner concludes that the vendor employee is the one that checks the logs and then restarts the logging process. Even if the Applicant disputes this, it is clear that someone associated with the vendor, initiates the logging of data. Therefore the Examiner does not believe he has improperly characterized Circenis."

The Examiner also states on page 10 of the present Office Action that Circenis teaches "[t]he iCOD computer could save usage data to a log file or a central metering device that a vendor employee could check periodically by visiting the site". The Examiner further states that the Examiner "*interprets the vendor employee as the user the (sic) indicates logging is desired*".

The Applicants respectfully suggest that this argument made by the Examiner now fails in view of the amendment made to claim 1 discussed above. Furthermore, the Applicants respectfully suggest that the Examiner is improperly reading Circenis well beyond the scope of Circenis. For example, the teaching of "[t]he vendor would likely want a method for accounting and auditing usage to ensure that the customers were not tampering with the CPU usage data" at paragraph [00023] of Circenis does not suggest that a vendor employee restarts the logging process once the employee checks the log. Nowhere does Circenis suggest that the vendor initiates logging. Nowhere does Circenis suggest that the vendor has access to a customer's system. The vendor merely configures an application to performing a monitoring operation. This monitoring operation runs every time a customer uses an application. Circenis does not suggest that monitoring stops and is restarted by a vendor. The teaching of "[t]he vendor would likely want a method for accounting and auditing usage to ensure that the customers were not tampering with the CPU usage data" does not suggest any of the conclusions made by the Examiner. Accordingly the presently claimed invention distinguishes over Circenis for at least these reasons as well.

The Examiner correctly states on page 5 of the present Office Action that

> "Circenis does not explicitly teach an encryption system which generates at least one symmetric key and encrypts the log entry for the at least one set of data using the symmetric key, wherein the encryption system encrypts the symmetric key using a public key associated with the encryption system, wherein the log file includes the symmetric key which has been encrypted with the public key."

However, the Examiner goes on to state:

"PGP ("Pretty Good Privacy") is a program that provides cryptographic privacy and authentication, and was created by Phillip Zimmermann in 1991. The OpenPGP standard (1998) is cited, but any PGP product teaches the generic method of:

1. Creating a message
2. Generating a symmetric key to be used as a session key for the message
3. Encrypting the session key using each recipient's public key. These "encrypted session keys" start the message.
4. The sending PGP encrypts the message using the session key, which forms the remainder of the message.
5. The receiving PGP device decrypts the session key using the recipient's private key
6. The receiving PGP decrypts the message using the session key."

Circenis individually or in combination does not teach the claim elements discussed above and claims elements discussed below.

The Examiner correctly states on pages 6-7 of the present Office Action that Circenis and PGP "do not explicitly teach a log file of a relatively-fixed size which stores the log entry for the at least one set of data which have been encrypted". However, the Examiner combines Circenis and PGP with the IBM reference to overcome the deficiencies of Circenis and PGP. In particular, the Examiner states that the IBM reference teaches:

> "a log file of a relatively-fixed size which stores the log entry for the at least one set of data which have been encrypted; ("The alog command can maintain and manager logs. It reads standard input, writes to standard output, and copies the output into a fixed-sized file. This file is treated as a circular log" Section 2.4.1.)"
>
> "a system for wrapping around and filling the log file from a beginning when the log file has been filled, allowing the log file to remain at a substantially-constant size even after the log file has been filled with data and a new entry is received. ("If the file is full, new entries are written over the oldest existing entries" Section 2.4.1). It is inherent that a circular log will wrap around and fill the log file from a beginning when the log file has been filled."

The Examiner also correctly states that Circenis and the IBM reference do not explicitly teach "random data in the log file when it is originally created and which is replaced by log entries so

that a size of the log including log entries appears to by a substantially-constant size". The Examiner goes on to state "It would have been obvious to one or ordinary skill in the art at the time of the invention to insert random data into the log file when it is initially created. The motivation is to initialize the circular log."

The Applicants respectfully disagree with the Examiner's interpretation of the IBM reference. As discussed in the previous Response With Amendment, it is not customary to always insert random data into log files. Second, fixed-size files do not have to be initialized with random data. A fixed-sized file such as that taught by the IBM reference can be defined as a file that cannot exceed a certain size. For example, if the file is fixed at 100 bytes, the file can comprise any number of bytes from 0 to 100, but not exceed 100 bytes. The presently claimed invention, on the other hand, inserts random data into the log file at its creation so that the log file appears to be a substantially constant size no matter how many log entries are in the log file.

The Applicants are unsure on how the Examiner concludes that a circular file, as taught by the IBM reference, is always populated with random data when created. As discussed above, a circular file can have a maximum size associated with it and when this maximum size is reached ,old data is re-written, thereby creating a circular file. In fact, the IBM reference states that "the alog file...is a cyclic file so, when its size gets to the maximum, it is overwritten". This clearly shows that the circular file of the IBM reference is not populated with random data when it is generated and is only set to a maximum file size.

Therefore, the inherency argued by the Examiner does not exist. If the presently claimed element is inherent and obvious, then the Applicants respectfully request that the Examiner provide references teaching "...a log file of a relatively-fixed size which stores the log entry for the at least one set of data which has been encrypted, and wherein the log file includes the symmetric key which has been encrypted with the public key; random data in the log file when it is originally created and which is replaced by log entries so that a size of the log file including log

entries appears to be a substantially constant size..." Accordingly, claim 1 (and similarly claims 10, 15, and 20) distinguishes over Circenis alone and/or in view of the IBM reference.

For the foregoing reasons, Claims 1-22 distinguish over Circenis alone and/or in combination with the IBM reference. Claims 2-9, 11-14, 16-19, and 21-22 depend from claims 1, 10, 15, and 20, respectively. Since dependent claims include all the limitations of the independent claims, claims 2-9, 11-14, 16-19, and 21-22 distinguish over Circenis alone and/or in combination with the IBM reference, as well. Accordingly, Applicants believe that the rejection under 35 U.S.C. § 103(a) has been overcome and respectfully request that this rejection be withdrawn.

CONCLUSION

Applicants acknowledge the continuing duty of candor and good faith to disclosure of information known to be material to the examination of this application. In accordance with 37 CFR § 1.56, all such information is dutifully made of record. The foreseeable equivalents of any territory surrendered by amendment is limited to the territory taught by the information of record. No other territory afforded by the doctrine of equivalents is knowingly surrendered and everything else is unforeseeable at the time of this amendment by the Applicants and their attorneys.

Applicants respectfully submit that all of the grounds for rejection stated in the Examiner's Office Action have been overcome and that all claims in the application are allowable. No Previously Presented matter has been added. It is believed that the application is now in condition for allowance or alternatively is in better form for consideration on appeal, which allowance is respectfully requested.

The Commissioner is hereby authorized to charge any fees that may be required or credit any overpayment to Deposit Account 09-0460. In view of the preceding discussion, it is submitted that the claims are in condition for allowance. Reconsideration and re-examination is requested.

PLEASE CALL the undersigned if that would expedite the prosecution of this application.

Respectfully Submitted,

Date: January 2, 2008

/Jon A. Gibbons/
Attorney for the Applicants
Jon A. Gibbons
(Reg. No. 37,333)

Fleit, Kain, Gibbons, Gutman,
Bongini & Bianco P.L.
551 N.W. 77th Street, Suite 111
Boca Raton, FL 33487
Telephone No.: (561) 989-9811
Facsimile No.: (561) 989-9812